



2366 Eastlake Ave. East

Suite 311

Seattle, WA 98102

o. 206.723.1941

f. 206.260.3031

48 North Pleasant St.

Suite 304

Amherst, MA 01002

o. 413.253.2700

f. 413.253.2702

ww
act

July 6, 2010

Via Email (john.wack@nist.gov and uocava-voting@nist.gov)

Technical Guidelines Development Committee
and Its UOCAVA Working Group
c/o National Institute of Standards and Technology
100 Bureau Drive, Building 101
Gaithersburg, Maryland 20899-8900

Comments for July 8-9, 2010 TGDC meeting and to Security
Considerations for Remote Electronic UOCAVA Voting, Draft White
Paper for the TGDC (by TGDC UOCAVA Working Group), regarding
Internet Voting and EAC proposed UOCAVA pilot program voting
system testing and certification requirements and manual

Dear Technical Guidelines Development Committee:

For consideration at your recently announced July 8-9, 2010 meeting regarding UOCAVA voting, Voter Action submits with this letter, as Exhibit A, its April 26, 2010 comments to the Election Assistance Commission (EAC) regarding EAC proposed federal requirements to govern federal testing and certification of Internet voting systems, for use in pilot programs by uniformed and overseas voters to cast their votes in at least the 2010 federal election. As explained in Voter Action's April 26, 2010 comments, the EAC did not follow its and your committee's enabling legislation, the Help America Voter Act (HAVA), or other federal law, in developing the Uniformed and Overseas Absentee Voter Act (UOCAVA) pilot program voting system testing and certification requirements and a related manual. Moreover, the EAC proposed requirements and manual, if adopted by the EAC, are less stringent than the Voluntary Voting System Guidelines applicable to all voting systems, and yet these new standards are required to meet the heightened risks posed by Internet voting to election integrity. Since the EAC appears to be moving forward with its proposed requirements and manual, this letter refers you to our April 26, 2010 letter,¹ and provides you, in the following paragraphs and related exhibits, with developments since April 26, 2010. This letter is, thus, as a supplement to the April 26, 2010 letter, and provides new information that further compels the conclusion that the TGDC should not endorse or acquiesce to the EAC proposed

¹ A copy of the April 26, 2010 Letter from Voter Action to the EAC is attached as Exhibit A. The letter and its exhibits are posted at the EAC website, the link to which is http://www.eac.gov/comments/testing_and_certification_comments.aspx (click under the name John Bonifaz). Voter Action's April 26, 2010 and all other exhibits to this letter are incorporated by reference into this letter.

requirements and manual. The proposed requirements and manual should not be adopted, but instead should be withdrawn from consideration by the EAC.²

To be clear, Voter Action supports the use of the Internet to deliver ballots to military and overseas voters, which the federal agency responsible for administering UOCAVA, the Federal Voter Assistance Program (FVAP) of the Department of Defense, is working to provide this year. What FVAP is not providing for the 2010 federal election,³ and about which Voter Action is concerned, is any voting system that uses the Internet, whether by email, web applications, or web-based fax and phone, to deliver ballots that are marked with votes.

The recent developments addressed in this letter are (1) federal charges against voting systems company Diebold and its former chief executive officer Walden W. O'Dell with fraud, during the years in which Diebold made, sold and serviced voting systems, and in which O'Dell wrote a letter in which he said he would deliver Ohio for then-President George Bush in the 2004 Presidential Election; (2) the potential malfunction or corruption of paperless touchscreen voting systems made by ES&S, for years the largest voting systems company in the United States, in the 2010 Democratic primary in South Carolina on June 8, 2010, in which an unknown candidate with no campaign won the U.S. Democratic primary for the U.S. Senate seat now held by Republican Jim DeMint; (3) the swift rise this spring of Dominion, a little-known foreign company engaged in Internet voting and with no reported income, to become the first or second largest voting machine company in the United States, after purchasing, in May 2010, voting systems made by Diebold (Diebold formerly was the second largest voting systems company in the U.S. and no longer has a U.S. voting systems business), and after purchasing, in June 2010, Sequoia Voting Systems, the voting machines of which rely on proprietary source code developed and owned by Smartmatic, a company headquartered in Venezuela with ties to the Hugo Chavez government of Venezuela, and (4) the movement of cyber security legislation to the U.S. Senate floor as cyber warfare from foreign nations and persons accelerates.

Before turning to describe briefly these recent developments, we will first bring to your attention to a report issued last week by the US Public Policy Committee of the Association of Computing Machinery, the largest association of computer programmers and specialists.

² At this meeting, the TGDC apparently will be asked to consider "charging" its UOCAVA Working Group to "examine guidelines developed for the EAC's manned kiosk pilot program and assist in developing further guidelines for addition pilot pilots." See <http://www.nist.gov/lit/vote/upload/UOCAVA-WG-Report.ppt#374,3>, Charge to the Working Group. The "guidelines developed for the EAC's manned kiosk pilot program" have been proposed, but have not been adopted, by the EAC. Nor should they be adopted by the EAC for the reasons stated in this and the April 26, 2010 letter of Voter Action, including the fact that these guidelines were developed for the EAC not by the TGDC, as required by HAVA. Voter Action also submits these comments to the UOCAVA Working Group of the TGDC, in response to requests for comments to Security Considerations for Remote Electronic UOCAVA Voting, Draft White Paper for the TGDC, http://www.nist.gov/itl/vote/upload/draft.UOCAVA_security_considerations-june2010.doc. See <http://www.nist.gov/itl/vote/draft-wp-securityconsiderations.cfm>. TGDC UOCAVA Working Group notes from the group's last meeting indicate that its work is not directed to the 2010 elections. See http://www.vote.nist.gov/workinggroups/UOCAVA_WG-6-2-10.doc.

³ FVAP is providing blank ballots to military and overseas voters to be returned by mail. See April 15, 2010 comments by FVAP to the EAC, posted at http://www.eac.gov/comments/testing_and_certification_comments.aspx (click under the name Joe Rothschild); Voter Action comments to EAC, http://www.eac.gov/comments/testing_and_certification_comments.aspx (click under the name John Bonifaz); Tom Reisen, Pentagon Hopes Online Balloting Boosts Overseas Voting, National Journal.com (May 3, 2010), <http://burnafterreading.nationaljournal.com/2010/05/pentagon-hopes-online.php>.

USACM recommends against the use of un-auditable Internet connected voting systems for voted ballots.

I. No Un-auditable Internet Voting, Declares USACM

About a week ago, the U.S. Public Policy Council of the Association for Computing Machinery published an Issue Brief entitled: “Internet Voting and Uniformed and Overseas Citizens Absentee Voters.”⁴ The ACM brief is short should be read in full.⁵ We excerpt some key points here.

A major challenge of internet voting (and of any form of electronic voting) is that there is no known way to confidently audit electronic voted ballots, including ballots generated by email, fax, or phone voting. This is because of a fundamental difference between voting and commerce. While fraudulent transactions occur in commerce, we eventually detect them, because commercial transactions create records that are checked by the people who are allegedly the originators of the transactions. *Election theft is much harder to detect, because there is only one transaction per person, and that person has no way to later audit his or her vote.*

If no reliable post-election audit or recount is conducted, then incorrect software or malicious code could result in the wrong candidate being declared the winner. . . .

According to a December 2009 report from the Computer Security Institute, a survey of 443 companies and government agencies found that 64% had reported malware infections (malicious software such as viruses or worms) in the preceding year. . . .

Election stealing software on a voter's computer can cast a ballot independent of the voter's intention, and the voter will never know. The computer screen will accurately reflect the voter's choice, but the malware can modify the voter's vote before it is sent over the internet. In other words, *it is the malware that votes*, not the voter.

[T]he companies that produce internet voting software or process internet-based votes are not safe. News reports of government and corporate sites being hacked are becoming more frequent. In a March 2010 talk, FBI Director Robert Mueller is quoted as saying that the FBI's computer network had been penetrated and that the attackers

⁴ The ACM is the world's largest - at 90,000 members strong - educational and scientific computing society, uniting computing educators, researchers and professionals to address the field's challenges. USACM, “Issue Brief: Internet Voting and Uniformed and Overseas Citizen Absentee Votes, U.S. Public Policy Council of the Association for Computing Machinery, at pages 6-7 (June 2010), usacm.acm.org/usacm/PDF/IB_Internet_Voting_UOCAVA.pdf.

⁵ USACM, “Issue Brief: Internet Voting and Uniformed and Overseas Citizen Absentee Votes,” U.S. Public Policy Council of the Association for Computing Machinery (June 2010), usacm.acm.org/usacm/PDF/IB_Internet_Voting_UOCAVA.pdf.

had “corrupted data.” The same article discussed the recent successful Google attack, which targeted Google intellectual property, as well as Gmail accounts of Chinese human rights activists:

Researchers investigating the Google attack -- thought to have affected at least 100 companies including Intel, Adobe and Symantec -- say that *prime targets of the hackers were the source code management systems used by software developers to build code.*

The implication of Mueller’s comments and the Google attack is that *voting system software could be rigged by outsiders, including attackers from another country.* (The Google attack appears to have originated in China). Another disturbing aspect of the attack targets is that Symantec, one of the targeted companies, is a major supplier of anti-virus and anti-spyware software. *The attacked companies, which employ large numbers of computer security experts, have vastly more resources than the relatively small internet voting vendors.*

While *external risks from hackers is significant, insider risks should not be ignored.* As demonstrated by rogue trader Jerome Kerviel, charged with losing about \$7 billion in unauthorized transactions at Société Générale by exploiting his insider status, a malicious trusted insider can be a major threat. Such an insider could hide election-stealing software in large software programs used by vendors and web- based voting sites. If the malware were cleverly hidden, detection could be very difficult.

Paperless kiosk voting has many of the same risks as undedicated internet voting. These include malware infections, denial of service attacks, coercion, and threats to the voter's privacy that jeopardize his right to a secret ballot. While the risks of phishing attacks and vote selling are significantly reduced by the use of a kiosk, *the accuracy and security threats, including the possibility that an insider might rig the machine, make paperless kiosk voting unacceptable.*

While returning voted ballots over the internet could improve access and responsiveness for UOCAVA voters, *internet voting introduces dangerous risks that can allow elections to be undetectably altered by malicious attacks or buggy software.*

Without paper ballots, it is impossible to conduct a post-election audit or recount of the internet votes.

*Elections are a fundamental component of our national security, and they must be treated as such. Introducing new voting methodologies into real elections demands rigorous risk assessment to ensure the most fundamental election property: integrity.*⁶

⁶ USACM, “Issue Brief: Internet Voting and Uniformed and Overseas Citizen Absentee Votes,” U.S. Public Policy Council of the Association for Computing Machinery (June 2010) (emphasis added), usacm.acm.org/usacm/PDF/IB_Internet_Voting_UOCAVA.pdf.

II. Voting System Business Diebold and Its Former CEO Settle Charges of Fraud.

On June 2, 2010, the federal Security and Exchange Commission announced a settlement with Diebold and its former Chief Executive Officer, Walden O'Dell on charges of fraud. The charges brought by the SEC concerned accounting fraud and were resolved by Diebold and O'Dell, without admission of liability, through payment of \$25 million and over \$ 1.5 million, respectively and other remedies.⁷

During the same time period of the frauds alleged by the SEC, 2002-2007, Diebold rose to be the second largest voting machine company in the United States and repeatedly came under suspicion of election irregularities and fraud.⁸ Diebold entered into the voting systems business in 2002 with the passage of HAVA and its provision of billions of federal funds to pay for new voting systems across the country. In August 2003, Walden O'Dell wrote a letter in which he declared that he would deliver Ohio, the state in which Diebold is based and in which Diebold voting systems would be used in the 2004 Presidential election, to then-President George Bush, for whom he was a major fundraiser. Diebold voting systems were thereafter found to use uncertified software and to be easily hacked. In September 2009, Diebold sold its U.S. voting systems business (by then renamed Premier Election Solutions) to its largest competitor, ES&S, for a modest \$5 million, after having tried to sell the business for some three years.⁹

Diebold may be out of the U.S. voting systems business but its apparent lack of integrity in its business operations illustrates the need for strong measures to protect against election fraud by, or made possible by, election insiders. Insider fraud poses an exponentially greater threat to election integrity if insiders can access elections statewide or nationwide via the Internet.

III. Potential Fraud or Voting Machine Malfunction At Issue in June 8, 2010 U.S. Senate Democratic Primary Election in South Carolina

⁷ Zachary Goldfarb, "Diebold Settles Fraud Charges for \$25 million," Wash. Post A13 (June 3, 2010), <http://www.washingtonpost.com/wp.dyn/content/articles/2010/06/02/AR2010060204509.html>; *see also* SEC v. Diebold, CA No: 1:10-cv-00908 (PLF)(D.D.C. June 2, 2010), and SEC v. Walden W. O'Dell, CA No: 1:10-cv-00909 (PLF) (D.D.C. June 2, 2010), available on PACER for a fee.

⁸ Kim Zetter, "Diebold Unloads Beleaguered Voting Machine Division," Wired (Sept. 3, 2009), <http://www.wired.com/threatlevel/2009/09/diebold-sells/>; Melanie Warner, Machine Politics in the Digital Age, NY Times (Nov. 9, 2003), <http://www.nytimes.com/2003/11/09/business/yourmoney/09vote.html>; Editorial, The Business of Voting, NY Times (Dec. 18, 2005), <http://www.nytimes.com/2009/09/10/opinion/10thu2.html>.

⁹ Kim Zetter, "Diebold Unloads Beleaguered Voting Machine Division," Wired (Sept. 3, 2009), <http://www.wired.com/threatlevel/2009/09/diebold-sells/>; Melanie Warner, Machine Politics in the Digital Age, NY Times (Nov. 9, 2003), <http://www.nytimes.com/2003/11/09/business/yourmoney/09vote.html>; Editorial, The Business of Voting, NY Times (Dec. 18, 2005), <http://www.nytimes.com/2009/09/10/opinion/10thu2.html>; Ohio Evaluation & Validation of Election-Related Equipment, Standards & Testing (EVEREST) Report, <http://www.sos.state.oh.us/elections/voterInformation/equipment/VotingSystemReviewFindings.aspx>; California Top-to-Bottom Review, www.sos.ca.gov/voting-systems/oversight/to-t-bottom-review.htm; Susan Pynchon, "The Harri Hursti Hack and its Importance to our Nation, Florida Fair Elections Coalition, VoterTrustUSA (Jan. 21, 2006), http://www.votetrustusa.org/index.php?option=com_content&task=view&id=798&Itemid=51; Veronica Dagher, "Diebold Drops Out of the U.S. Voting Machine Business, Wall St. J. (Sept. 4 2010), <http://online.wsj.com/article/SB125199401359883707.html>; Pete Yost, "Justice Department Investigating Diebold's Sale of Voting Machine Subsidiary," AP, Ohio.com (Akron Beacon Journal (Mar. 4, 2010), http://webcache.googleusercontent.com/search?q=cache:_sITnRDB_D4J:www.ohio.com/business/86341622.html+Diebold+second+largest+voting+machines+company&cd=11&hl=en&ct=clnk&gl=us.

The 2010 U.S. Senate Democratic Primary in the South Carolina is under investigation by federal¹⁰ and state¹¹ authorities, is the subject of federal litigation¹² and led to a candidate's protest.¹³ Alvin Greene, an unknown, unemployed defendant in a criminal case and represented until now by a public defender due to his claimed indigency, paid \$10,000 to become a candidate in the U.S. Senate Democratic Primary in South Carolina, neither campaigned nor fundraised, and is now the current Democratic nominee for the U.S. Senate seat now held by Republican Jim DeMint.¹⁴

At the center of the disputed 2010 U.S. Senate Democratic primary election in South Carolina are paperless touchscreen voting machines. As has been reported in the press, there is a substantial disparity between the results of the absentee vote count and the primary day vote count. Unlike the election day voters who used the paperless touchscreen voting machines,¹⁵ most absentee voters marked their votes on papers ballots that were thereafter tabulated by optical scanner equipment. Victor Rawl, who reportedly lost the South Carolina Democratic Primary for the US Senate to Alvin Greene, submitted hours of evidence, including the testimony of experts, taking issue with the vote count from the electronic touchscreen voting machines.¹⁶ The voting machines at issue are Electronic Systems and Software (ES&S) iVotronics, which have been involved in prior anomalous election results, including the 18,000 undervotes registered in a close congressional election between Christine Jennings and Vern Buchanan in November 2006 in Sarasota, Florida.¹⁷ The South Carolina Democratic Primary

¹⁰ In the Matter of Alvin M Greene et al, Federal Election Commission, June 15, 2010 (Citizens for Responsibility and Ethics in Washington Complaint against Alvin M. Greene), Exhibits and Letter from the FEC to CREW acknowledging complaint and opening of proceeding (June 22, 2010), available at <http://www.citizensforethics.org/node/45307>.

¹¹ Alvin Greene Probe Underway: South Carolina Senate Candidate Faces Investigation, Huffington Post, AP (June 28, 2010), http://www.huffingtonpost.com/2010/06/28/alvin-greene-probe-underw_n_628043.html; Kris Alingod, South Carolina Begins Probe of Democratic Candidate Alvin Greene (Jun. 29, 2010), <http://gantdaily.com/2010/06/29/south-carolina-begins-probe-of-democratic-candidate-alvin-greene/>.

¹² Bursey v. South Carolina State Election Commission, CA 3:10-cv-01545-CMC (June 16, 2010) (Complaint including Affidavit and Exhibits).

¹³ Statement by the Vic Rawl for US Senate Campaign, "South Carolina would rather be 100% rights than 90% uncertain," Vic Rawl for Senate (June 2010), <http://www.vicrawl.com/vicrawl/post/1002-statement-by-the-vic-rawl-for-us-senate-campaign>; Rebecca Abrahams, South Carolina Democratic Party Denies Rawl's Protest, Huffington Post, June 18, 2010, http://www.huffingtonpost.com/rebecca-abrahams/south-carolina-democratic_b_616775.html; Tony Santaella, Alvin Greene Primary Win Over Vic Rawl Upheld by Democratic Committee, wltx.com, June 18, 2010, <http://www.wltx.com/news/story.aspx?storyid=88697>.

¹⁴ Rob Grove, "Doubt grows in South Carolina election results, examiner (June 15, 2010.), <http://www.examiner.com/x-44755-Charleston-County-Elections-2010~y2010m6d15-Doubt-grows-in-South-Carolina-election-results>, and citations in preceding footnotes 10-13.

¹⁵ The iVotronic "uses an electronic ballot system with no auditable voter-verified record of votes." Kathy Dopp, "South Carolina 2010 Democratic United State Senate Primary Election," Abstract (Jun 15, 2010) (attached as an exhibit to the Bursey v. South Carolina State Election Commission complaint).

¹⁶ Rebecca Abrahams, South Carolina Democratic Party Denies Rawl's Protest, Huffington Post, June 18, 2010, http://www.huffingtonpost.com/rebecca-abrahams/south-carolina-democratic_b_616775.html; Tony Santaella, Alvin Greene Primary Win Over Vic Rawl Upheld by Democratic Committee, wltx.com, June 18, 2010, <http://www.wltx.com/news/story.aspx?storyid=88697>.

¹⁷ Bob Mahlburg and Maurice Tamman, "Dist. 13 voting analysis shows broad problem," *HeraldTribune.com* (Nov. 9, 2006), <http://www.heraldtribune.com/article/20061109/NEWS/611090343>.

illustrates the need for auditable and re-countable paper ballots to check against election fraud and abuse.¹⁸

IV. Dominion, Now the Largest or Second Largest Voting System Company, Is Foreign Controlled and Depends Upon Secret Source Code Created and Owned by Smartmatic, a Foreign Controlled Company With Ties to The Venezuelan Government Led by Hugo Chavez

Privately-held Canadian voting system company Dominion¹⁹ in the past few weeks has purchased (1) Diebold voting systems from ES&S, and (2) Sequoia Voting Systems.²⁰ These purchases reportedly make Dominion the largest or second largest voting system company in the United States.²¹ Dominion is reported by Dun & Bradstreet to be a Toronto-based company with one listed key official, board members and employee, John Poulos, and under \$18 million in sales for which the company obtains no income.²²

On May 19, 2010, Dominion announced its purchase of Diebold voting systems from ES&S and on June 28, 2010, a federal court required ES&S to sell voting systems assets that ES&S purchased from Diebold to resolve an antitrust suit brought by the United States against ES&S.²³ According to Dominion's press release,²⁴ Premier voting systems are currently in use in over 1,400 jurisdictions in 33 states and serve nearly 28 million American voters." Of the deal, John Poulos, the President, CEO and Director of Dominion declared: "We are extremely pleased to conclude this transaction, which will restore much-needed competition to the American voting systems market and will allow Dominion to expand its capabilities and operational footprint to every corner of the United States."²⁴

¹⁸ Barbara Zia, "Voting Machines Deserve a Second Look," The State (June 27, 2010).). Cf "ATM security flaws could be a jackpot for hackers," Reuters (June 25, 2010), <http://www.thestate.com/2010/06/27/1350698/zia-voting-machines-deserve-second.html>.

¹⁹ Dominion Voting System Corporation, Bloomberg Businessweek, <http://investing.businessweek.com/research/stocks/private/snapshot.asp?privcapId=46054856>.

²⁰ Press Releases, Dominion Voting Systems, Inc. Acquires Premier Election Solutions Assets From ES&S, *Transaction Approved by the U. S. Department of Justice, Will Significantly Increase Competition in the United States Voting Systems Industry, Dominion's Engineering and Customer Service Expertise Will Support Premier's Voting Products Throughout the U.S.* (May 19, 2010), <http://www.dominionvoting.com/images/pdfs/DominionAcquiresPremierReleaseFinal4.pdg>, and Dominion Voting Systems Corporation Acquires Assets of Sequoia Voting Systems *Transaction Further Expands Dominion's Geographic Reach; Retention of Sequoia Employees and Acquisition of Facilities Will Assure Seamless Transition for Current Sequoia Customers* (June 4, 2010), <http://www.dominionvoting.com/images/pdfs/DominionAcquiresSequoiaFinal.pdf>.

²¹ "Exclusive: On Heels of Diebold/Premier Purchase, Canadian E-Voting Firm Dominion Also Acquires Sequoia, Lies About Chavez-Ties in the Announcement, 'Intellectual Property' of voting systems still owned by firm linked to Venezuelan President, despite press statement to the contrary, PLUS: The election official/e-voting company revolving 'oversight' door continues to turn..., bradblog.com (June 21, 2010), <http://www.bradblog.com/?cat=442>.

²² Hoovers, Dominion Voting Systems Corporate Profile (July 1, 2010), available for purchase from Hoovers, a Dun. & Bradstreet Company.

²³ Final Judgment, U.S. v. ES&S, CA No. 1:10 cv 00380 (JDB) (June 28, 2010); AP, Voting machine maker must sell some assets, Action 3 News (Omaha Nebraska) (July 1, 2010), <http://www.action3news.com/Global/story.asp?s=1274332&clienttype=printable>.

²⁴ Press Release, Dominion Voting Systems, Inc. Acquires Premier Election Solutions Assets From ES&S, *Transaction Approved by the U. S. Department of Justice, Will Significantly Increase Competition in the United States Voting Systems Industry, Dominion's Engineering and Customer Service Expertise Will Support Premier's Voting Products Throughout the U.S.* (May 19, 2010).

In a separate transaction announced on June 4, 2010, Dominion bought Sequoia Voting Systems, which is, according to Dominion, “a major U.S. provider of voting solutions serving nearly 300 jurisdictions in 16 states.” John Poulos of Dominion heralded this deal as “another important milestone in Dominion’s efforts to provide election officials in every region of the United States the widest array of comprehensive and innovative options when it comes to election solutions.”²⁵ Before the Sequoia acquisition, Dominion had worked with Sequoia in New York State for over three years, and had hired away one or more senior officials from Sequoia, including Edwin Smith, who now is a member of the Technical Guidelines Development Committee.²⁶

Dominion represents that, “as part of the transaction, Dominion has acquired Sequoia’s inventory and all intellectual property, including software, firmware and hardware.” But Sequoia could only sell to Dominion that which it owns. When Smartmatic sold Sequoia to an investment group led by Sequoia’s management team,²⁷ during an investigation by the Committee on Foreign Investment in the United States (CFIUS)²⁸ into the identity of the person(s) who ultimately own Smartmatic and its ties to the Chavez government,²⁹ Smartmatic apparently retained ownership of the software used in Sequoia voting systems to cast and count votes, licensing to Sequoia that software, which Smartmatic develops in Venezuela.³⁰

²⁵ Press Release, Dominion Voting Systems Corporation Acquires Assets of Sequoia Voting Systems Transaction Further Expands Dominion’s Geographic Reach; Retention of Sequoia Employees and Acquisition of Facilities Will Assure Seamless Transition for Current Sequoia Customers (June 4, 2010).

²⁶ Press Release, New Technical and Scientific Experts Appointed to EAC’s Technical Guidelines Development Committee, Election Assistance Commission, (Dec. 11, 2009), <http://www.electionexcellence.org/home/63-eac-news/216-new-technical-and-scientific-experts-appointed-to-eacs-technical-guidelines-development-committee.html>.

²⁷ While the terms of the Sequoia sale by Smartmatic in late 2007 were not made public, the Sequoia press release states that the sale transaction includes a loan and an earn-out from Smartmatic. Press Release, Sequoia Voting Systems, U.S. Voting Technology Leader Sequoia Voting Systems Announces New Corporate Ownership (Nov. 8, 2007), <http://www.nacrc.org/PressReleases/2007/SequoiaSaleRelease110807.pdf>.

²⁸ CFIUS is a U.S. Government inter-agency committee led by the U.S. Department of Treasury that addresses national security risks posed by foreign ownership of or influence over U.S. business, including companies providing the means by which voters in the U.S. election their President and Congressional Representatives. 50 U.S.C. App. § 2170(a); *see also* 31 C.F.R. § 800 App. A.

²⁹ “On December 22, 2006, Smartmatic Corporation announced the company’s intention to sell Sequoia Voting Systems, given the difficult climate in the United States marketplace, tainted by a non-stop debate against foreign investment, especially in the election technology area,” Press Release, Smartmatic Announces Sale of Subsidiary Sequoia Voting Systems (Nov. 8, 2007), <http://www.smartmatic.com/pressroom/view/article/smartmatic-announces-the-sale-of-its-subsiary-sequoia-voting-systems/>; Press Release, Smartmatic Announces Sale of Sequoia Voting Systems, Rep. Maloney Shined Congressional Spotlight on Questionable Deal, Helped Enact Tough Reforms to Strengthen Oversight of Foreign Investment (Nov. 8, 2007), http://maloney.house.gov/index.php?option=com_content&task=view&id=1491&Itemid=61.

³⁰ Letter Opinion of Apr. 4, 2008, *Smartmatic Corp. v. SVS Holdings, Inc. and Sequoia Voting Systems, Inc.*; and *SVS Holdings, Inc. and Sequoia Voting Systems, Inc. v. Smartmatic Corp. and Hart InterCivic, Inc.*, Civil Action No. 3585-VCL, pages 13-14, *available at* http://bradblog.com/Docs/SVSSequoia_v_Hart_Smartmatic_Lamb_Decision_040408.pdf. At the time of this opinion about ten Smartmatic employees worked in the company’s Boca Raton, Florida office, the vast majority of its employees, indeed more than one hundred of them, work in Venezuela, including members of Smartmatic’s computer design and research and development staff. *See* Dun & Bradstreet Report on Smartmatic (2008), *report available for purchase at* <http://www.db.com/us/>. For additional information, see attached memorandum entitled “Sequoia Voting Systems, Inc. Uses Vote-Counting Software Developed, Owned, and Licensed By Foreign-Owned Smartmatic, A Company Linked to the Venezuelan Government of Hugo Chavez,” Voter Action, June 12, 2008.

Efforts to date have not succeeded in determining the ultimate owners of Smartmatic or the extent to which Smartmatic and the Chavez government of Venezuela have influence over U.S. elections through Smartmatic's control of the software that counts votes for Sequoia (now Dominion) voting machines. Concern is that Smartmatic's sale of Sequoia "was fraudulent,"³¹ "a sham transaction designed to fool regulators."³²

Dominion apparently will employ Venezuelan-run Smartmatic's propriety software in at least the Sequoia voting systems that it now owns. Dominion also is engaged in Internet voting outside the United States,³³ and could employ Venezuelan-run Smartmatic's propriety software in Internet voting in U.S. elections.

Not only is it not known who owns and controls Smartmatic, we do not know who owns and controls privately-held and Canadian-based Dominion. Does Dominion owe Smartmatic on the Sequoia loan or earn-out? How was Dominion able to finance these Diebold and Sequoia purchases? Who is going to finance Dominion's work through the November 2010 election?³⁴

V. Cybersecurity Legislation to Senate Floor as Cyber Warfare Threatens U.S.

On June 24, 2010, the Senate Homeland Security and Governmental Affairs Committee unanimously reported out of committee The Protecting Cyberspace as a National Asset Act of 2010, S. 3480. This legislation would create, among other things, a White House Office of Cyberspace Policy "to lead federal and private sector efforts to secure critical cyber networks and assets. "Catastrophic cyber attack is no longer a fantasy or a fiction," said Senator Lieberman, a sponsor of the legislation; "it is a clear and present danger."³⁵ According to another sponsor, Senator Collins, "computer systems in Executive Branch agencies and in congressional agencies are now under attack an average of 1.8 billion times a month. . . . And intelligence officials have warned over and over again that these attacks are becoming more and more sophisticated." A third sponsor, Senator Carper declared that "[o]ver the past few decades, our society has become increasingly dependent on the internet, including our military, government, and businesses of all kinds [and] while we have reaped enormous benefits from this powerful technology, unfortunately our enemies have identified cyber security as an ideal 21st century battlefield."

Earlier, on June 16, 2010, the General Accounting Office issued a report on cybersecurity in which it declared that "cyber-based threats to federal systems and critical infrastructure are

³¹ Gerardo Reyes, *Voting machines firm ties to Venezuela questioned: A Chicago Alderman is not satisfied that a voting-systems company is free of influence from Venezuela President Hugo Chavez*, Miami Herald, Mar. 19, 2008, at 3 (article available for purchase at <http://www.miamiherald.com>).

³² Letter from Edward M. Burke, Chairman of the Chicago City Council Committee on Finance to Langdon D. Neal, Chairman, Chicago Board of Election Commissioners (Jan. 11, 2008), *available at* http://www.bradblog.com/Docs/SequoiaSmartmaticLetter_Chicago_EdBurkeToLangdonNeal_011108.pdf.

³³ A Comparative Assessment of Electronic Voting (excerpt on Canada), Elections Canada (February 2010), <http://elections.ca/content.asp?section=loi&document=municip&dir=res/ivote/comp&lang=e&textonly=false>

³⁴ According to Hoover's, Dominion dates back to 2003, about the time Congress enacted HAVA, and, by letter dated February 1, 2007, the Election Assistance Commission welcomed Dominion to its voting system testing and certification program, http://www.eac.gov/testing_and_certification/manufacturers_registered_in_the_program.aspx.

³⁵ "Committee Adopts Comprehensive Cybersecurity legislation," Homeland Security and Governmental Affairs Committee press release (June 24, 2010), http://hsgac.senate.gov/public/index.cfm?FuseAction=Press.MajorityNews&ContentRecord_id=6be6b903-5056-8059-76ef-7e691cc176fd.

evolving and growing. These threats can come from a variety of sources, including criminals and foreign nations. . . . [C]yber attackers do not need to be physically close to their targets, their attacks can easily cross state and national borders, and cyber attackers can easily preserve their anonymity. Further, the interconnectivity between information systems, the Internet, and other infrastructure presents increasing opportunities for such attacks.”³⁶

Between fiscal years 2006 and 2009, reports of security incidents from federal agencies has increased 400 percent, to 30,000 incidents in 2009. The leading types of incidents reported were (1) malicious code, that is software that infects an operating system or application, (2) unauthorized access, that is, where an person gains logical or physical access to a system without permission.³⁷

On the television talk show “This Week,” which aired on June 27, 2010, CIA Director Leon Panetta said in response to the question as to what threat the U.S. is not paying enough attention: cyber warfare. “We are now in a world in which cyber warfare is very real. It could threaten our grid system. It could threaten our financial system,” Panetta said. “It could paralyze this country, and I think that’s an area we have to pay a lot more attention to,” the CIA chief said.”³⁸

The Internet was designed for convenience and reliability, *not security*,” reiterates the Economist in this week’s cover story: “Cyberwar: The threat from the internet.”³⁹ “Growing connectivity over the insecure internet multiplies the avenues for e-attack. . . . Steven Chabinsky, a senior FBI official responsible for cyber-security, recently said that “given enough time, motivation and funding, a determined adversary will always – always – be able to penetrate a targeted system.”⁴⁰ According to Greg Day of McAfee, a vendor of IT security products, “[h]acking used to be about making noise. Now it’s about staying silent. . . . Hackers have become wholesale providers of malware – viruses, worms and Trojans that infect computers –for others to use. . . . Malware is typically used . . . to open a ‘backdoor’ to a computer so that it can be taken over by outsiders. . . . The next step after penetrating networks to steal data is to disrupt or manipulate them. If military targeting information could be attacked, for example, ballistic missiles would be useless. Those who play war games speak of being able to ‘change the red and blue dots’: make friendly (blue) forces appear to be the enemy (red), and vice versa.”⁴¹ The dots switched from red to blue or vice versa could just as easily be the votes cast for candidates in a Presidential or other election in the United States.

Appearing before the Election Assistance Commission earlier this year, a “CIA cybersecurity expert suggested that Venezuelan President Hugo Chavez and his allies fixed a 2004 election recount,” reports the press. The expert, Steve Stigall, remarked that “I follow the vote. And

³⁶ “Continued Attention Is Needed to Protect Federal Information Systems from Evolving Threats,” June 16, 2010, GAO-10-834T, at introduction., <http://www.gao.gov/new.items/d10834t.pdf>.

³⁷ “Continued Attention Is Needed to Protect Federal Information Systems from Evolving Threats,” June 16, 2010, GAO-10-834T, at pages 3 and 4, <http://www.gao.gov/new.items/d10834t.pdf>.

³⁸ “Cyber warfare could paralyze US,” <http://blogs.abcnews.com/politicalpunch/2010/06/cia-cyber-warfare-could-paralyze-us.htm>.

³⁹ Cyberwar War in the fifth domain Are the mouse and keyboard the new weapons of conflict?, The Economist, pages 25-26 (July 3-9, 2010), <http://www.economist.com/node/16478792>.

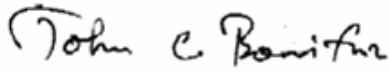
⁴⁰ Cyberwar War in the fifth domain Are the mouse and keyboard the new weapons of conflict?, The Economist, pages 25-26 (July 3-9, 2010), <http://www.economist.com/node/16478792>;

⁴¹ Cyberwar War in the fifth domain Are the mouse and keyboard the new weapons of conflict?, The Economist, pages 26-28 (July 3-9, 2010), <http://www.economist.com/node/16478792>

wherever the vote becomes an electron and touches a computer, that's an opportunity for a malicious actor potentially to . . . make bad things happen” Stigall reportedly told the EAC that “voting equipment connected to the Internet could be hacked, and machines that weren't connected could be compromised wirelessly. Eleven U.S. states have banned or limited wireless capability in voting equipment, but Stigall said that election officials didn't always know it when wireless cards were embedded in their machines. Stigall’s presentation reportedly “undercut calls by some U.S. politicians to shift to Internet balloting, at least for military personnel and other American citizens living overseas. Stigall said that most Web-based ballot systems had proved to be insecure.”⁴²

For the reasons stated in Voter Action’s April 26, 2010 comments to the EAC regarding its proposed UOCAVA pilot program voting system testing and certification requirements and manual, and for the reasons stated in this letter, and the exhibits referenced in these letters, the EAC Technical Guidelines Development Committee should recommend against EAC adoption of the EAC proposed UOCACA requirements and manual.

Sincerely,



John C. Bonifaz
Encls.

cc: Donetta Davidson, Election Assistance
Commission, Chair
Gracia Hillman, Commissioner
Gineen Bresso Beach, Commissioner
Thomas R. Wilkey, Executive Director
Tamar Nedzar, Associate General Counsel
Brian Hancock, Director of Voting System Certification

⁴² Greg Gordon, Most Electronic Voting Isn’t Secure, CIA Expert Says (Mar. 29, 2009), <http://www.electionexcellence.org/home/26-media/118-most-electronic-voting-isnt-secure-cia-expert-says.html>